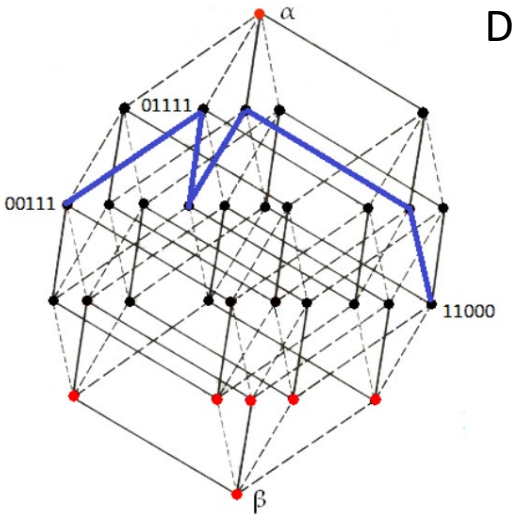
University of Puerto Rico Mayaguez Campus
Faculty of Arts and Sciences
Department of Mathematical Sciences
call box 9000, Mayagüez, P.R. 00681

THE DEPARTMENT OF MATHEMATICAL SCIENCES PROUDLY PRESENTS

# COLLOQUIUM

Setiembre 12, 2024

## Characterization and affine equivalence of k-rotation symmetric Boolean functions.




Dr. Jose E. Calderón
**UPR-Mayaguez**

**Setiembre 12-2024**
**10:45 am**
**Monzón 201**

Rotation symmetric Boolean functions were introduced by Pieprzyk and Qu in 1999. They proved that these functions have efficient and secured cryptographic implementations. Later, in 2007, Kavut and Yucel found a function that exceed the Bent concatenation bound in this new class of functions. Concepts such as affine equivalence, Hamming weight, and nonlinearity have been studied for small degrees. In this talk we give an explicit characterization of generators of k-rotation monomial Boolean functions. These generators can be used to determine when a k-rotation monomial is a short cycle or a long one. We also use such generators to count the number of cycles for a given value of the degree and a given value of length. We also present a study on the affine equivalence of such monomials to determine whenever two k-rotation monomials are affine equivalent.

Ph.D. in CISE
University of Puerto Rico